

# セキュア・コーディング・ガイドライン

## 脆弱性を修正および回避するための実践的なガイダンス

開発者が「バグの山」を取り除けるように、通常の一般的なコーディング規則に具体的で実用的な修正アドバイスを加えています。

## セキュア・コーディング・ガイドラインが必要な3つの理由

### 1. 開発者をパワーアップする

ブラック・ダックの実用的な総合ガイドラインは開発者が書いた開発者のためのもので、テクノロジー別のリスク説明、ベストプラクティス、再利用可能なコードサンプルが記載されています。開発者がセキュアなソフトウェアを作成し、脆弱性のバックログを解消するために必要なフレームワーク、ライブラリ、言語別のアドバイスを提供します。また、お客様自身の修正に関するベストプラクティスを追加することで、独自のセキュリティのベストプラクティスに効果的に対応できるようになります。

### 2. 標準コーディング手法で効率が向上する

ブラック・ダックのセキュア・コーディング・ガイドラインには、セキュリティ要件を作成するための設計図が記載されており、開発者はテスト済みの手引きをもとに社内標準を確立できるようになります。これにより組織全体で一貫したコーディング標準を使用できるようになります。

### 3. すぐに効果がでる

セキュア・コーディング・ガイドラインによって、開発者にセキュアなソフトウェアの作成方法を示すことで、コストがかかり、時間の無駄となる不具合の数を最小限に抑えます。また簡単に展開して利用できるのも、メリットがすぐに認められます。

## フレームワークと言語

- .Net
- C/C++
- COBOL
- JAVA
- Java Web Services
- MEAN
- Ruby on Rails
- Web 2.0 (HTML5, JavaScript)
- PHP

## 必要な専門知識、ツール、サービスを提供します

このガイドラインは 23 年以上に及ぶブラック・ダックのソフトウェア・セキュリティのノウハウを集約し、業界標準の最適な情報源を加えたものです。また、脆弱性と修正手法の進化に合わせて内容が最新になるよう社内研究にも継続的に投資しています。

セキュアコーディング標準の対応範囲は以下のテーマ領域です。

- セキュアな入力処理
- セキュアな出力処理
- アクセス制御
- セキュアなセッション管理
- セキュアなデータ転送と保存

## カスタマイズ手法

必要に応じて、以下に対応するためガイドラインをカスタマイズします。

- 対象の開発言語やフレームワークの追加
- 発見された脆弱性種別の追加
- 独自の社内セキュリティフレームワーク
- 社内コーディング標準の統合

## ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。詳しくは [www.blackduck.com/jp](http://www.blackduck.com/jp) をご覧ください。

### ブラック・ダック・ソフトウェア合同会社

[www.blackduck.com/jp](http://www.blackduck.com/jp)

©2024 Black Duck Software, Inc. All rights reserved. Black Duck® は Black Duck Software, Inc. の米国およびその他の国における登録商標です。その他の会社名および商品名は各社の商標または登録商標です。2024 年 9 月